STAFF SUMMARY SHEET

	TO	ACTION	SIGNATURE (Surname), GRADE AND DATE		TO	ACTION	SIGNATURE (Surname), GRADE AND DATE
1	DFMI Dept Head	Approve	Lt Col, 12 Mar 13	6			
2	DFER	Review	Texas, GL 1 Mar 13	7		Grammar typos	
3	DFMI	Action		8			
4				9			
5				10			

SURNAME OF ACTION OFFICER AND GRADE	SYMBOL	PHONE	TYPIST'S INITIALS	SUSPENSE DATE
Dr Talbot, AD-24	DFMI	333-9425	bt	

SUBJECT	DATE
Clearance of Material for Public Release USAFA-DF-PA-180-185	20120308

SUMMARY

1. PURPOSE: To provide security and policy review of the attached documents prior to public release.

2. BACKGROUND: Cadets Joshua Huckabee, Gordan Lang, Joseph Shields, Branden Shoenfeld, and Vincent Jovene were Military and Strategic Studies majors enrolled in our department's MSS 498 capstone course and their essays in this issue of Airman Scholar Journal represent their senior thesis work from Spring 2012. The final article is a book review by Cadet Edward Boylan, an MSS student in a senior core course. Note that the first article in this issue (Thomas Drohan, "Core Relevance at the Air Force Academy)" was previously cleared for public release for a conference presentation in 2011.

Titles: 2) "Active Learning and the Rising Generation of Air Force Officers," 3) "Hands on Keyboard: Considerations for a Cyber Weapons School," 4) "Siezing the Ultimate High Ground: Weaponizing Space," 5) "An Airplane for all Seasons," 6) "Personnel Recovery: CV-22 Expansion Pack;" and 7) a book review of "War Made New."

Issue overview: Cadet Joshua Huckabee argues for improved simulation scenarios in the Cadet Battle Lab, DFMIs premier networked classroom. Cadet Gordan Lang follows with his proposal for a joint military cyber school to train the rising generation of cyber warriors. Cadet Joseph Shields argues the merits of weaponizing space. Cader Brandon Shoenfeld argues that the Air Force should purchase the A-29 Super Tuscano over the AT-6 Texan II built by a US-based company, and interestingly, the Air Force just announced the A-29 as it's choice, validating Brandon's argument. Cadet Vincent Jovene also make an airframe argument for Combat Search and Rescue, advocating the purchase of CV-22 Osprey's to augment the HH-50 rescue fleet. Lastly, our book review by Cadet Edward Boylan covers a primary text used in MSS 416, in which he was enrolled as a Humanities major.

Release Information: release for web-based publication in the e-journal entitled: Airman Scholar Journal (ASJ)

Recommended Distribution Statement: Distribution A, Approved for public release, distribution unlimited.

3. RECOMMENDATION: Sign Approve/Review blocks above indicating documents are suitable for public release. Suitibility is based solely on the document being unclassified, not jeapordizing DOD interests, nor inaccurately portraying official policy.

B Talbot

Brent J. Talbot, PhD
Professor and Director of Research
Department of Military Strategic Studies

HANDS ON KEYBOARD

CONSIDERATIONS FOR A CYBER WEAPONS SCHOOL

GORDON LANG

The United States Air Force has recently taken great strides in establishing an effective cyber warfare component. Nevertheless, there remains a significant amount of work to fully integrate the cyber mission into the institutional Air Force. That effort includes the need for a well-developed Cyber Weapons School (CWS) to provide graduate level training and serve as the Air Force's cyber training flagship organization. The question this paper attempts to answer is how this proposed Air Force Cyber Weapons School should be structured in order to develop highly effective network warfare specialists.

Networks and cyberspace are crucial in nearly every current Air Force mission and can be expected to have an increasing role to play in the future. For example, Remotely Piloted Vehicles (RPVs) in current conflicts are assuming combat roles; the link connecting the plane to its pilot halfway across the world is entirely within the cyberspace domain. As the Air Force increases its RPV inventories and expands their roles, peoples' lives and the success of the mission could hinge on the security of the link between RPV and pilot. Other operations, such as intelligence gathering, information security, defense of energy grids, and surface to air missile targeting are all highly integrated into cyberspace networks.[1]

There is currently a cyber training squadron attached to the Air Force Weapons School at Nellis Air Force Base, but given the major focus and culture at Nellis, cyber operators likely are not primary focus of attention, and their mission calls goes beyond the traditional battlespace.[2] While the Weapons School at Nellis is focused on, "achieving battlespace dominance" in a typical kinetic warfare sense, there are many functions of network warfare that operate independently of physical battles.[3] This traditional focus of the Weapons School at Nellis could marginalize uniquely cyber missions at the expense of assisting kinetic operations.

This essay provides an alternative possibility to remedy this issue. It is concerned with developing a basic blueprint, or outline, for how this new, or rejuvinated CWS should be developed. Various academic issues will be addressed, such as the content and length of the curriculum and how best to achieve the overall objectives of this education. This study is not intended to provide a detailed, lesson-by-lesson syllabus for the school.

This paper will offer a number of contentions. First, the proposed Cyber Weapons School does not have to be built completely from scratch. Three current weapons schools will be evaluated in an effort to find a ready-made baseline on which to model the new CWS: the Air Force Weapons School, the Navy's Top Gun, and the Army Ranger School. Each of their basic frameworks will be drawn upon; in particular, curriculum content, teaching techniques, as well as standards for evaluating and managing students. Second, the major unique dimension of cyber operations will be considered; i.e., the fact that almost every new attack involves methods even an experienced operator has not yet seen. It will be argued that the solution to this problem requires that the CWS must promote independent, quick, and intelligent decision-making by its students. In order to achieve these important outcomes,

Cadet GORDON LANG is a Military & Strategic Studies major in the Class of 2012.

a general outline of the CWS program will be offered. What is envisioned is a three month-long course that addresses all three subsets of cyber operations in an environment that is stressful and mirrors what operations against an intelligent and capable enemy might actually look like.

Like an infantryman, a cyber operator conceivably could be engaged in continuous combat for extended periods. Ranger School simulates this by creating an overarching war game-type mission within which the students must function. The Air Force Cyber Weapons School should take a similar approach.

Similarities of the CWS to Current Weapons Schools

Weapons schools are nothing new to the United States military so there is no need to start from scratch when designing a Cyber Weapons School. The Air Force's Weapons School, the Navy's Top Gun, and the Army's Ranger School all have practices which, when properly employed, can create a ready-made, strong foundation on which to build a CWS. Its focus would be providing the experience and tools needed by cyber operators to become the leading experts in their home squadrons once they return. Because the CWS would not have the opportunity to train the entire career field due to operational and monetary concerns, as well as the pre-requisite experience required for admission, graduates would be expected to share their newfound knowledge. The Air Force Weapons School tells its students to, "'make others like you,' spreading the wealth of experience, leadership skills and knowledge."[4] The Navy and the Army also promote this concept of "training the trainer," an idea that can be leveraged in the cyber community to great effect. Cyber operations are one of the fastest changing fields in the military and new ideas and methods are constantly required to remain competitive. By leveraging CWS graduates as prime-instructors within their own squadrons, more people can be exposed to the various ideas and practices that will make the graduates the best in their field. This approach would encourage open-mindedness and promote a system of a bottom-up meritocracy of ideas in which the best become the most used rather than a having single school's syllabus dominating the field for better or worse.

Another dimension of the CWS modeled after its more kinetic counterparts would be its focus on practical applications of theory. While an undergraduate course may be more concerned with how to best use the weapons and materials given to the operator, a weapons school should be more concerned with how those weapons actually work. This is exemplified by how the Navy went about creating Top Gun: the initial instructors "wanted to teach the Top Gun crews how the [Sparrow] missile worked and therefore 'how they could successfully deploy it.'"[5] In the classroom-based theory section of the CWS curriculum, emphasis should be placed on understanding how the various network warfare techniques and tools work. Using this fundamental understanding of how their tools operate, network warfare specialists would be well equipped to devise their own methods of operation and adapt quickly to a changing environment. Coupled with the expectation that graduates will help train, either formally or informally, members of their operational squadrons, it would also discourage a culture of expecting the weapons to work "like magic" within the cyber operations community.

The theory and engineering behind cyber operations are important to understand, but in order to fight best in cyberspace specialists must comprehend the connection between theory and actual operations. While the academic side should be modeled after the Air Force and Naval Weapons schools, the practical side should be based on the Army's Ranger school. This is because Top Gun was designed around, "training hops [that] were designed... to test the crew's ability to do all these [dog-fighting maneuvers] in a quick and efficient manner,"[6] while the Ranger School is more with concerned creating a long term, continuous training environment.[7] Like an infantryman, a cyber operator conceivably could be engaged in continuous combat for extended periods. Ranger School simulates this by creating an overarching war game-type mission within which the students must function. The Air Force CWS should take a similar approach. By linking all the exercises together, a fictional cyber war can be created, allowing the instructors to create the most realistic "worst case" scenario for a cyber conflict. CWS

graduates must experience and be able to handle the accompanying stress in a manner similar to that of successful Ranger School students, something that the Air Force and Naval Weapons schools do not place emphasis on.

Officers do not dominate network warfare. The enlisted force also has an important part to play in operating systems. To best educate selected members of this force the CWS cannot be officer-exclusive as both aviation weapons schools are, and instead must accept enlisted students as well. This may pose problems for an Air Force-run Weapons School, which so far have not been expected to train enlisted personnel. To best deal with the challenge, the Army's methods of training their enlisted force in advanced courses should be used as a framework. For example, there is "no rank in Ranger School;" rather, everyone is given opportunities in leadership positions and are evaluated based on a common rubric for all students.[8] This principle should also be extended to instructors, who must be selected for their outstanding proficiency and teaching capacity rather than the rank they happen to hold.

Established weapons schools also have an air of being reserved for the elite. The high dropout rates of Ranger School are well established at around 50 percent per class, including recycled students.[9] Graduates of the Weapons School at Nellis Air Force Base have a special patch they wear and are categorized as "patch wearers." To be successful, the CWS must also have an elite culture and reputation. Its graduates should be viewed as a brotherhood of the best cyber operators in the world. In large part this can be achieved through the standard methods currently in use at the established weapons schools. More specifically, the CWS must offer a comprehensive and very challenging course both, in theory and practical application. It should also have a strict selection process for potential students, as well as a system for evaluating CWS students and the authority to disenroll or recycle underperformers. CWS instructors should be military members, the very best operators in their community, and already have graduated from the Weapons School themselves.[10]

Graduates should be authorized an outward symbol of their achievement, most easily accomplished through the use of a patch they can wear on their operational uniform. Additionally, the instructors, and perhaps the students, should work to achieve a mythos of being legendary men and women, while realizing that many cyber-accomplishments will never be known outside the classified community. Ideally, attending the Cyber Weapons School would be more than career advancing; it would also be a rite of passage.[11]

Special Considerations

Cyberspace operations are unique in that they are far-and-away the fastest form of operations currently available. Richard Clark writes that, "Cyber war happens at the speed of light... the time between the launch of an attack and its effect is barely measurable, thus creating risks for crisis decision makers."[12] Other missions, bound by the requirement to employ large pieces of physical equipment and Newtonian physics, are inherently slower than their cyber counterparts. Accordingly, the nature of cyber conflict requires that its operators be exceptionally quick thinking, intelligent, and independent in order to succeed in such a unique environment. These are all qualities generally assumed to be necessary for combat officers, but in the cyber realm such qualities also must be possessed by enlisted members. A Cyber Weapons School should not only have both officer and enlisted students, but would also require a syllabus that is focused on developing fast, independent, and critically thinking warfighters. Students should not be provided set solutions or structured scenarios as is often the case with the established weapons schools at which, for example, a certain airframe can use the same maneuver on an

enemy time and again and always claim victory because of the different limitations of each aircraft.[13] In cyberspace, where every actor has the same capabilities and can execute any "maneuver" they wish, there cannot be prescribed solutions to specific problems. Instead, students must be taught to think quickly and creatively while operating effectively against unique threats.

Once a cyber operator has encountered a specific type of enemy action they should be able to effectively negate it through experience, as "exploits tend to depreciate rapidly after exposure; i.e., first time use."[14] This means that for an attack to be most effective it should be what is called a "zero-day" threat; that is, a program or exploit that has not yet been used. These threats, and their counters, can be thought of as analogous to the common cold. Consider: while a cold causes the same symptoms every time, ones' body is still vulnerable to them even after decades of living because the virus changes how it is structured, and can then pass by the body's defenses unnoticed and achieve its "mission." Computer operations are generally intended to cause some sort of effect from an established list, but if an operator uses the exact same attack tactic repeatedly, it will be met with rapidly depreciating results, just as a biological virus that does not change its appearance would experience. As such, the school's curriculum must be able to rapidly evolve to include current events, new threats and, most importantly, ensure that no two classes are provided the same scenarios. If a graduate was able to pass along a schedule of training events to a current student, the CWS would have lost its ability to train outside-the-box, independent, quick thinkers.

A Snapshot of the proposed Cyber Weapons School

One basic question concerns the length of the course at the Cyber Weapons School. The US Army Ranger school takes two months to train its students.[15] The Air Force Weapons School takes six.[16] A dedicated CWS would be much more like Ranger school in this regard as unlike Air Force Weapons School students, CWS students would only be required to learn about cyber operations. Also, due to the quickly evolving nature of cyber operations, the school cannot be so long that its lessons become obsolete before graduation. The complicated math and engineering involved in advanced cyber activities is yet another factor, as it would take more than just a basic run-through to achieve the desired level of understanding. With these three factors considered, the CWS should ideally have a curriculum of roughly three months. While the initial cyber attack and defense course, known as Intermediate Network Warfare Training (INWT), is nine weeks, this is only long enough to prepare novice operators for their new job.[17] For a critical in-depth understanding of the cyber mission, extra time will have to be allocated. A three-month-long syllabus should be sufficient to achieve such a level of understanding. Three months would also be long enough to achieve the desired social effects of camaraderie and to stress the students while still being short enough to hopefully, avoid becoming obsolete.

Because graduates of the CWS would be the absolute best network warfare specialists in the Air Force, they have to be well versed in every aspect of their career field. In all, there are three core specialties of cyberspace operations that must be covered in this school: computer network attack, defense, and exploitation.[18] Network attack involves actively hampering enemy computer operations, exploitation is the collection of information, and defense is securing friendly networks against the previous two operations.[19]

While these competencies could be divided up equally by allocating one month of training to each, that would not be the best way to structure the material. Continuously teaching new concepts and applications, and expecting the students to master and employ them all in practice, would make for a more challenging course, facilitate smoother transitions between subjects, and offer a more realistic experience. By covering the theories behind each type of operation as well as practicing their application, the students would not only become adept at their particular mission, but would also better understand the actions of their opponents and thus be more likely to mitigate them effectively. A deep understanding of all the cyber missions would also enable graduates to become operators and leaders in any network warfare squadron, enabling the spread and diffusion of knowledge while still retaining maximum mission effectiveness.

In the INWT course students are taught a wide range of subjects intended to prepare them for their new job as network warfare specialists, including "policy,

doctrine, employment, executing organizations and missions, operational functions, and law and ethics."[20] In comparison, the CWS would be one month longer and focus solely on how to best execute missions based on the assumption that students would already have an acceptable grasp of subjects such as cyber law and morality. Included in the CWS curriculum would be instruction on the theoretical and technical workings of cyber operations, much as current weapons schools teach how a particular missile functions so as to best employ or counter it. For CWS students, this would mean not just learning which operation to use when, but how each part of the weapon, or computer program, functions. By understanding their operational tools on an intimate level, the students would not be confined to using premade programs or standard missions. Instead, they would be able to tailor their actions to meet a specific challenge as well as more quickly conceive of ways to combine their mission's tools for novel effects. The basics of which type of attack to use when and the knowledge of what to look for during a defensive or exploitation mission is taught at INWT and through job experience. The purpose of the theoretical instruction portion of the CWS would be to understand the inner workings of those capabilities, in which the operator would not have the time or the knowledge to learn independently.

The CWS program also would include practical exercises, which would constitute much of the curriculum. Students would be expected to leverage both their own experiences and classroom instruction to devise and execute network warfare operations in realistic scenarios. Overarching conflict scenarios, similar to Red Flag or the Ranger School's Aragon Liberation Front setting, would provide a backdrop against which to frame the training in a realistic way. There should be at least two teams for each scenario, perhaps with additional factions being added to further complicate the situation in later simulations. The instructors, because of their significant experience and skill, should take an active part in opposing the students in their assigned missions, but this should not be the only method of identifying teams. Student-on-student missions would expose exercise participants to even more variations of attack and defense, as would having instructors act as team leaders from time to time. These various types of student-instructor team combinations would expose the students to a greater number of different personalities and operational preferences, thereby giving them as much experience as is possible.

War-gaming events should also be relatively ill defined. Students should only receive a mission or desired end state and then be told to achieve it. Greater learning takes place when a problem is imposed without a known solution, as the students will not know what will be directed at them by the opposing team. Only by using quick, intelligent thought and action will they win. This, in turn, will encourage the students not only to understand the material but to think for themselves. Similar scenarios are set up at Red Flag for cyber operators, where the red and blue teams battle each other through networks.[21] However, the CWS would go a step further than Red Flag. Students should not be told when or under what circumstances the scenario ends. That, coupled with twenty-four hour operations and multiple shifts, would present as realistic an environment as possible. Rather than just a regular school day, forcing the students to operate effectively in situations where they have high stress and no fixed end date would help further facilitate the types of learning and experience that CWS seeks to promote.

If CWS students are to learn effective cyber operations, they will require instructors who can understand and teach the material. These instructors should be the best operators the network attack and defense communities have to offer. They should have significant say in what particular lessons the syllabus includes, as they would be the best qualified to know what is important and what is not with respect to cyber operations. They would be best equipped to identify who is not preforming up to standards or not putting forth the required effort in a way that standardized tests and objectives could not. Subsequently, CWS graduates, both officers and enlisted, would naturally become the primary pool for future instructors. Spending a tour as a teacher at the CWS would be very similar to a tour at other weapons schools in that such individuals would be identified as exceptional candidates for senior leadership positions and special duties.

Findings and Conclusions

There are many common features shared by weapons schools.

All of the existing schools expect their graduates to return to their units and teach others what they have learned. In this way, a larger audience can be reached without unduly taxing readiness or the weapons school's limited staff. Understanding the link between theoretical, classroom-based instruction and its implementation in realistic scenarios is also a common feature of all weapons schools. A major difference, though, is that while the Air Force school trains only officers, the CWS must include significant numbers of enlisted troops. The Army's Ranger School can provide direction on how to approach this problem as it holds that all rank is equal among Ranger candidates.

As noted above, cyber conflict differs from the other missions that currently are examined in existing weapons schools. In the case of cyber operations, there are never set, unchanging methods of operations. While a fighter pilot can learn how to defeat a particular airframe or missile with a high likelihood of success every time afterwards, network warfare specialists should expect to routinely find themselves confronted with attack techniques they have never seen before. Addressing this, the CWS should not focus on teaching prescribed solutions or set answers, but should instead seek to develop an intelligent, quick, and independent operator who can rapidly comprehend and perform effectively in unique scenarios.

The CWS's curriculum should focus on both the theory and practice of each of the three primary subsets of network warfare operations: attack, defense, and exploitation. Rather than examining these missions separately, they should be studied in an integrated fashion that would provide both a tougher learning environment and more realistic scenarios. The classroom portion of the CWS would involve teaching the workings of the cyber environment as well as the tools used to complete missions that the operator may encounter. The main goal should be to give students the ability to create new capabilities based on their personal deep understanding. Most of the course should be spent in war gaming-type activities. Designed to be as realistic as possible, involving multiple teams, no checklists, an undisclosed end date, and twenty-four hour operations, these exercises should be designed to test the student's capability to effectively fight in a contested battle space against a sophisticated enemy.

Instructors should be drawn from the very best specialists in the network warfare community as they will be the ones who will develop the syllabus and run this premier cyber training unit. Rank should not be a factor when selecting faculty, just as it should not be a factor when selecting students. Once enrolled, the students should expect to be treated equally, regardless of specialty or rank, in order to encourage the best possible learning environment. Constant adjustment of exercise scenarios would also be necessary to reach the desired outcomes. If a set pattern of operations can be identified and shared among generations of students, then the CWS will lose its ability to surprise, which is crucial to the desired training outcomes. Additionally, a dynamic curriculum will enable the proposed CWS to stay abreast of advancing technologies and new threats, providing students with the most relevant education possible.

A three-month course at the CWS would be sufficient to achieve all of these objectives. Students are only expected to learn about the various capabilities within cyber operations. Accordingly, the CWS does not need to last six months like the Air Force Weapons School, which requires its students to learn and understand every type of mission performed by the Air Force. Three months is also long enough to significantly stress the students, testing their abilities even in the worst of situations, while remaining short enough to minimize the possibility of instructional content becoming obsolete before the students graduate. Finally, the CWS should be promoted as the premier Air Force school for cyber warfare training. In addition to all the factors described above, an identification symbol, most likely a cyber weapons patch, should be awarded to graduates as is currently the case at Nellis, which is the cyber-equivalent of the fighter weapons school patch. The "patch wearers" of the flying world are considered the best airmen, and the proposed Cyber Weapons School mentioned herein intends the same end result, to train and educate the best cyber-warriors.

---

1 Cyber warfare, or computer network warfare, describes the missions carried out in the cyber domain. It is the use of computer networks and cyber assets to conduct attack, defense, and exploitation missions against an enemy's networks. The United States military describes it as the operation and use of the "global information grid;" the combined networks, software, services, and information connected to cyberspace. Joint Publication (JP), 1-02,

Department of Defense Dictionary of Military and Associated Terms, 12 April 2001 as amended through 31 July 2010, 143, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

2 The Air Force Weapons School is six months long, and includes students from every type of airframe as well as the intelligence, space, missile, services, and cyber communities; all of which are expected to learn each other's missions and operations. The primary focus of the school is kinetic operations, and support for the kinetic mission.

3 J.R. Wilson, "DMN Q&A: Robert Garland, Commandant, USAF Weapons School," Defense Media Network, http://www.defensemedianetwork.com/stories/qa-with-col-robert-shark-garland-commandant-usaf-weapons-school/

4 Ibid.

5 Robert K. Wilcox, Scream of Eagles: The Creation of Top Gun – And the US Air Victory in Vietnam (New York: John Wiley & Sons, Inc., 1990), 145.

6 Ibid, 146.

7 "Ranger Training Brigade: US Army Ranger School," Fort Benning, Georgia, http://www.benning.army.mil/infantry/rtb/content/PDF/Ranger%20School%20web11.pdf

8 Ibid.

9 Ibid.

10 Military members, as opposed to civilians or intelligence community people, are uniquely focused on the degradation and destruction of enemy assets, and are thus best suited for control of network warfare operations, and by extension the weapons school dedicated to it. Martin C. Libicki's book Cyberdetterence and Cyberwar, page 156, provides a more detailed explanation of this position.

11 Wilcox, 173.

12 Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It (New York: HarperCollins, 2010), 31.

13 Thomas Lang, interview by author, February 28, 2012.

14 Martin C. Libicki, Cyberdeterrence and Cyberwar, (Santa Monica, CA: RAND Corporation, 2009), 157.

15 "Ranger Training Brigade..."

16 Wilson.

17 Scott McNabb, "Initial cyber INWT class graduates schoolhouse," 24th Air Force, http://www.24af.af.mil/news/story.asp?id=123251064

18 Joint Publication (JP), 3-13, Information Operations, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf 34

19 Ibid.

20 Kinder Blacke, "Intermediate Network Warfare Training Up and Running," 24th Air Force, http://www.24af.af.mil/news/story.asp?id=123245134

21 Scott McNabb, "Red Flag Cyber Operations: Part II – Cyber Operators Stand Against Red Team 'Aggressors,'" Air Force Space Command, http://www.afspc.af.mil/news/story.asp?id=123246419

Raptor Flyover at Graduation